We claim:

1. A system for providing continuous authentication of a user of a computing device, comprising:

a security component which provides security functions, such that the security component can vouch for authenticity of one or more other components with which it is securely operably connected;

a biometric sensor component that is securely operably connected, as one of the one or more other components, to the security component;

securely-stored biometric information which identifies an owner of the computing device;

means for repeatedly obtaining, from the biometric sensor component, biometric input of a user of the computing device; and

means for comparing the repeatedly obtained biometric input to the securely-stored biometric information of the owner, wherein each of the comparisons comprises an authentication of the user.

2. The system according to Claim 1, wherein the means for repeatedly obtaining is activated upon beginning a security-sensitive operation and is terminated upon completion of the security-sensitive operation.

3. The system according to Claim 1, wherein the means for repeatedly obtaining is activated each time a predetermined time interval elapses.

4. The system according to Claim 3, wherein the predetermined time interval is selectively configured by the owner of the computing device.

5. The system according to Claim 1, wherein the means for repeatedly obtaining is activated upon switching between functions of the computing device.

6. The system according to Claim 1, wherein the means for repeatedly obtaining is activated upon switching between functions of an application that is executing a security-sensitive operation using the computing device.

7. The system according to Claim 1, wherein the means for repeatedly obtaining is activated when the biometric sensor component detects one or more of an interruption, change, or loss of the biometric input.

8. The system according to Claim 1, wherein the means for repeatedly obtaining is activated upon reaching one of at least one predetermined instructions in an application that is executing a security-sensitive operation using the computing device.

9. The system according to Claim 1, wherein the biometric sensor component is securely operably connected to the security component when the security component is manufactured.

10. The system according to Claim 1, wherein the other components comprise one or more of (1) input/output components and (2) application processing components.

11. The system according to Claim 1, wherein the means for securely operably connecting further comprises means for authenticating the biometric sensor component to the security component.

12. The system according to Claim 11, further comprising means for authenticating the security component to the biometric sensor component.

13. The system according to Claim 1, wherein the means for securely operably connecting is activated by a hardware reset of the biometric sensor component, and wherein the hardware reset is activated by operably connecting of the biometric sensor component.

14. The system according to Claim 11, wherein the means for authenticating the biometric sensor component is securely stored thereon.

15. The system according to Claim 11, wherein the means for authenticating further comprises means for using public key cryptography.

16. The system according to Claim 1, further comprising means for concluding that the user is the owner of the computing device only if the means for comparing succeeds.

17. The system according to Claim 1, wherein the biometric sensor component is a fingerprint sensor, and wherein the fingerprint sensor is capable of repeatedly obtaining a fingerprint of the user as the biometric input of the user while the computing device is being held by the user.

18. The system according to Claim 1, wherein the biometric sensor component is a retina scanner, and wherein the retina scanner is capable of repeatedly obtaining a retinal scan of the user as the biometric input of the user while the user is looking at the computing device.

19. The system according to Claim 1, wherein the means for comparing is performed by the biometric sensor component.

20. The system according to Claim 19, further comprising means for securely transferring the securely-stored biometric information of the owner to the biometric sensor component for use by the means for comparing.

21. The system according to Claim 1, wherein the means for comparing is performed by the security component.

22. The system according to Claim 2, further comprising means for aborting the security-sensitive operation if the means for repeatedly obtaining or the means for comparing fails to detect

the biometric information of the user, thereby causing the completion of the security-sensitive operation.

23. The system according to Claim 2, further comprising means for marking the security-sensitive operation as not authenticated if the means for repeatedly obtaining or the means for comparing fails to detect the biometric information of the user.

24. The system according to Claim 2, further comprising means for deactivating the computing device if the means for repeatedly obtaining or the means for comparing fails to detect the biometric information of the user.

25. The system according to Claim 2, further comprising means for concluding that the security-sensitive operation is authentic if the means for comparing succeeds until completion of the security-sensitive operation.

26. The system according to Claim 25, wherein the means for concluding that the security-sensitive operation is authentic also requires that all other components which are securely operably connected to the security core remain securely operably connected until completion of the security-sensitive operation.

27. The system according to Claim 25, wherein the means for concluding that the security-sensitive operation is authentic also requires that all other components which are securely

operably connected to the security core and which are involved in the security-sensitive operation remain securely operably connected until completion thereof.

28. The system according to Claim 11, wherein the means for authenticating further comprises means for performing a security handshake between the biometric sensor component and the security component.

29. The system according to Claim 11, wherein the biometric sensor component has associated therewith a unique device identifier that is used to identify data originating therefrom, a digital certificate, a private cryptographic key and a public cryptographic key that is cryptographically-associated with the private cryptographic key.

30. The system according to Claim 1, wherein the biometric sensor component is physically integrated with a card, and wherein a card reader adapted to reading the card is securely operably connected to the security component.

31. The system according to Claim 1 or Claim 30, further comprising:

previously-stored secrets of the owner of the computing device; and

means for accessing selected ones of the previously-stored secrets only if the means for comparing determines, over a duration of a security-sensitive operation, that the obtained biometric input of the user matches the securely-stored biometric information of the owner.

32. The system according to Claim 31, wherein the previously-stored secrets include a private cryptographic key of the owner, and wherein the means for accessing further comprises means for accessing the private key to compute a digital signature over information pertaining to the security-sensitive operation.

33. The system according to Claim 1, wherein the means for repeatedly obtaining is activated continually during an interval of a security-sensitive operation being performed with the computing device.

34. The system according to Claim 11, wherein the means for authenticating further comprises means for using (1) a unique identifier of the biometric sensor component, (2) a digital signature computed over the unique identifier using a private cryptographic key of the biometric sensor component, and (3) a public key that is cryptographically associated with the private key.

35. A method for providing continuous authentication of a user of a computing device, comprising steps of:

operating a security component which provides security functions, such that the security component can vouch for authenticity of one or more other components with which it is securely operably connected;

providing a biometric sensor component that is securely operably connected, as one of the one or more other components, to the security component;

providing securely-stored biometric information which identifies an owner of the computing device;

repeatedly obtaining, from the biometric sensor component, biometric input of a user of the computing device; and

comparing the repeatedly obtained biometric input to the securely-stored biometric information of the owner, wherein each of the comparisons comprises an authentication of the user.

36. The method according to Claim 35, wherein the step of repeatedly obtaining is activated upon beginning a security-sensitive operation and is terminated upon completion of the security-sensitive operation.

37. The method according to Claim 35, wherein the step of repeatedly obtaining is activated each time a predetermined time interval elapses.

38. The method according to Claim 37, wherein the predetermined time interval is selectively configured by the owner of the computing device.

39. The method according to Claim 35, wherein the step of repeatedly obtaining is activated upon switching between functions of the computing device.

40. The method according to Claim 35, wherein the step of repeatedly obtaining is activated upon switching between functions of an application that is executing a security-sensitive operation using the computing device.

41. The method according to Claim 35, wherein the step of repeatedly obtaining is activated when the biometric sensor component detects one or more of an interruption, change, or loss of the biometric input.

42. The method according to Claim 35, wherein the step of repeatedly obtaining is activated upon reaching one of at least one predetermined instructions in an application that is executing a security-sensitive operation using the computing device.

43. The method according to Claim 35, wherein the biometric sensor component is securely operably connected to the security component when the security component is manufactured.

44. The method according to Claim 35, wherein the other components comprise one or more of (1) input/output components and (2) application processing components.

45. The method according to Claim 35, wherein the step of securely operably connecting further comprises the step of authenticating the biometric sensor component to the security component.

46. The method according to Claim 45, further comprising the step of authenticating the security component to the biometric sensor component.

47. The method according to Claim 35, wherein the step of securely operably connecting is activated by a hardware reset of the biometric sensor component, and wherein the hardware reset is activated by operably connecting of the biometric sensor component.

48. The method according to Claim 45, wherein instructions to perform the step of authenticating the biometric sensor component are securely stored thereon.

49. The method according to Claim 45, wherein the step of authenticating further comprises the step of using public key cryptography.

50. The method according to Claim 35, further comprising the step of concluding that the user is the owner of the computing device only if the comparing step succeeds.

51. The method according to Claim 35, wherein the biometric sensor component is a fingerprint sensor, and wherein the fingerprint sensor is capable of repeatedly obtaining a fingerprint of the user as the biometric input of the user while the computing device is being held by the user.

52. The method according to Claim 35, wherein the biometric sensor component is a retina scanner, and wherein the retina scanner is capable of repeatedly obtaining a retinal scan of the user as the biometric input of the user while the user is looking at the computing device.

53. The method according to Claim 35, wherein the comparing step is performed by the biometric sensor component.

54. The method according to Claim 53, further comprising the step of securely transferring the securely-stored biometric information of the owner to the biometric sensor component for use by the comparing step.

55. The method according to Claim 35, wherein the comparing step is performed by the security component.

56. The method according to Claim 36, further comprising the step of aborting the security-sensitive operation if the step of repeatedly obtaining or the comparing step fails to detect the biometric information of the user, thereby causing the completion of the security-sensitive operation.

57. The method according to Claim 36, further comprising the step of marking the security-sensitive operation as not authenticated if the step of repeatedly obtaining or the comparing step fails to detect the biometric information of the user.

58. The method according to Claim 36, further comprising the step of deactivating the computing device if the step of repeatedly obtaining or the comparing step fails to detect the biometric information of the user.

59. The method according to Claim 36, further comprising the step of concluding that the security-sensitive operation is authentic if the comparing step succeeds until completion of the security-sensitive operation.

60. The method according to Claim 59, wherein the step of concluding that the security-sensitive operation is authentic also requires that all other components which are securely operably connected to the security core remain securely operably connected until completion of the security-sensitive operation.

61. The method according to Claim 59, wherein the step of concluding that the security-sensitive operation is authentic also requires that all other components which are securely operably connected to the security core and which are involved in the security-sensitive operation remain securely operably connected until completion thereof.

62. The method according to Claim 45, wherein the step of authenticating further comprises the step of performing a security handshake between the biometric sensor component and the security component.

63. The method according to Claim 45, wherein the biometric sensor component has associated therewith a unique device identifier that is used to identify data originating therefrom, a digital certificate, a private cryptographic key and a public cryptographic key that is cryptographically-associated with the private cryptographic key.

64. The method according to Claim 35, wherein the biometric sensor component is physically integrated with a card, and wherein a card reader adapted to reading the card is securely operably connected to the security component.

65. The method according to Claim 35, further comprising steps of:

providing previously-stored secrets of the owner of the computing device; and

accessing selected ones of the previously-stored secrets only if the comparing step determines, over a duration of a security-sensitive operation, that the obtained biometric input of the user matches the securely-stored biometric information of the owner.

66. The method according to Claim 65, wherein the previously-stored secrets include a private cryptographic key of the owner, and wherein the accessing step further comprises the step of accessing the private key to compute a digital signature over information pertaining to the security-sensitive operation.

67. The method according to Claim 35, wherein the step of repeatedly obtaining is activated continually during an interval of a security-sensitive operation being performed with the computing device.

68. The method according to Claim 45, wherein the step of authenticating further comprises the step of using (1) a unique identifier of the biometric sensor component, (2) a digital signature computed over the unique identifier using a private cryptographic key of the biometric sensor component, and (3) a public key that is cryptographically associated with the private key.

69. A computer program product for providing continuous authentication of a user of a computing device, the computer program product embodied on one or more computer-readable media and comprising:

computer-readable program code means for operating a security component which provides security functions, such that the security component can vouch for authenticity of one or more other components with which it is securely operably connected;

computer-readable program code means for accessing a biometric sensor component that is securely operably connected, as one of the one or more other components, to the security component;

computer-readable program code means for accessing securely-stored biometric information which identifies an owner of the computing device;

computer-readable program code means for repeatedly obtaining, from the biometric sensor component, biometric input of a user of the computing device; and

computer-readable program code means for comparing the repeatedly obtained biometric input to the securely-stored biometric information of the owner, wherein each of the comparisons comprises an authentication of the user.

70. The computer program product according to Claim 69, wherein the computer-readable program code means for repeatedly obtaining is activated upon beginning a security-sensitive operation and is terminated upon completion of the security-sensitive operation.

71. The computer program product according to Claim 69, wherein the computer-readable program code means for repeatedly obtaining is activated each time a predetermined time interval elapses.

72. The computer program product according to Claim 71, wherein the predetermined time interval is selectively configured by the owner of the computing device.

73. The computer program product according to Claim 69, wherein the computer-readable program code means for repeatedly obtaining is activated upon switching between functions of the computing device.

74. The computer program product according to Claim 69, wherein the computer-readable program code means for repeatedly obtaining is activated upon switching between functions of an application that is executing a security-sensitive operation using the computing device.

75. The computer program product according to Claim 69, wherein the computer-readable program code means for repeatedly obtaining is activated when the biometric sensor component detects one or more of an interruption, change, or loss of the biometric input.

76. The computer program product according to Claim 69, wherein the computer-readable program code means for repeatedly obtaining is activated upon reaching one of at least one predetermined instructions in an application that is executing a security-sensitive operation using the computing device.

77. The computer program product according to Claim 69, wherein the biometric sensor component is securely operably connected to the security component when the security component is manufactured.

78. The computer program product according to Claim 69, wherein the other components comprise one or more of (1) input/output components and (2) application processing components.

79. The computer program product according to Claim 69, wherein the computer-readable program code means for securely operably connecting further comprises computer-readable program code means for authenticating the biometric sensor component to the security component.

80. The computer program product according to Claim 79, further comprising computer-readable program code means for authenticating the security component to the biometric sensor component.

81. The computer program product according to Claim 69, wherein the computer-readable program code means for securely operably connecting is activated by a hardware reset of the biometric sensor component, and wherein the hardware reset is activated by operably connecting of the biometric sensor component.

82. The computer program product according to Claim 79, wherein the computer-readable program code means for authenticating the biometric sensor component is securely stored thereon.

83. The computer program product according to Claim 79, wherein the computer-readable program code means for authenticating further comprises computer-readable program code means for using public key cryptography.

84. The computer program product according to Claim 69, further comprising computer-readable program code means for concluding that the user is the owner of the computing device only if the computer-readable program code means for comparing succeeds.

85. The computer program product according to Claim 69, wherein the biometric sensor component is a fingerprint sensor, and wherein the fingerprint sensor is capable of repeatedly obtaining a fingerprint of the user as the biometric input of the user while the computing device is being held by the user.

86. The computer program product according to Claim 69, wherein the biometric sensor component is a retina scanner, and wherein the retina scanner is capable of repeatedly obtaining a retinal scan of the user as the biometric input of the user while the user is looking at the computing device.

87. The computer program product according to Claim 69, wherein the computer-readable program code means for comparing is performed by the biometric sensor component.

88. The computer program product according to Claim 87, further comprising computer-readable program code means for securely transferring the securely-stored biometric information of the owner to the biometric sensor component for use by the computer-readable program code means for comparing.

89. The computer program product according to Claim 69, wherein the computer-readable program code means for comparing is performed by the security component.

90. The computer program product according to Claim 70, further comprising computer-readable program code means for aborting the security-sensitive operation if the computer-readable program code means for repeatedly obtaining or the computer-readable program code means for comparing fails to detect the biometric information of the user, thereby causing the completion of the security-sensitive operation.

91. The computer program product according to Claim 70, further comprising computer-readable program code means for marking the security-sensitive operation as not authenticated if the computer-readable program code means for repeatedly obtaining or the computer-readable program code means for comparing fails to detect the biometric information of the user.

92. The computer program product according to Claim 70, further comprising computer-readable program code means for deactivating the computing device if the computer-readable program code means for repeatedly obtaining or the computer-readable program code means for comparing fails to detect the biometric information of the user.

93. The computer program product according to Claim 70, further comprising computer-readable program code means for concluding that the security-sensitive operation is authentic if the computer-readable program code means for comparing succeeds until completion of the security-sensitive operation.

94. The computer program product according to Claim 93, wherein the computer-readable program code means for concluding that the security-sensitive operation is authentic also requires that all other components which are securely operably connected to the security core remain securely operably connected until completion of the security-sensitive operation.

95. The computer program product according to Claim 93, wherein the computer-readable program code means for concluding that the security-sensitive operation is authentic also requires that all other components which are securely operably connected to the security core and which are involved in the security-sensitive operation remain securely operably connected until completion thereof.

96. The computer program product according to Claim 79, wherein the computer-readable program code means for authenticating further comprises computer-readable program code means for performing a security handshake between the biometric sensor component and the security component.

97. The computer program product according to Claim 79, wherein the biometric sensor component has associated therewith a unique device identifier that is used to identify data originating therefrom, a digital certificate, a private cryptographic key and a public cryptographic key that is cryptographically-associated with the private cryptographic key.

98. The computer program product according to Claim 69, wherein the biometric sensor component is physically integrated with a card, and wherein a card reader adapted to reading the card is securely operably connected to the security component.

99. The computer program product according to Claim 98, further comprising:

computer-readable program code means for accessing previously-stored secrets of the owner of the computing device; and

computer-readable program code means for accessing selected ones of the previously-stored secrets only if the computer-readable program code means for comparing determines, over a duration of a security-sensitive operation, that the obtained biometric input of the user matches the securely-stored biometric information of the owner.

100. The computer program product according to Claim 99, wherein the previously-stored secrets include a private cryptographic key of the owner, and wherein the computer-readable program code means for accessing further comprises computer-readable program code means for accessing the private key to compute a digital signature over information pertaining to the security-sensitive operation.

101. The computer program product according to Claim 69, wherein the computer-readable program code means for repeatedly obtaining is activated continually during an interval of a security-sensitive operation being performed with the computing device.

102. The computer program product according to Claim 79, wherein the computer-readable program code means for authenticating further comprises computer-readable program code means for using (1) a unique identifier of the biometric sensor component, (2) a digital signature computed over the unique identifier using a private cryptographic key of the biometric sensor component, and (3) a public key that is cryptographically associated with the private key.

103. A method of doing business by continually authenticating a user of a computing device, comprising steps of:

operating a security component for the computing device, wherein the security component provides security functions such that the security component can vouch for authenticity of one or more other components with which it is securely operably connected;

providing a biometric sensor component that is securely operably connected, as one of the one or more other components, to the security component;

providing securely-stored biometric information which identifies an owner of the computing device;

performing a security-sensitive operation using the computing device;

repeatedly obtaining, from the biometric sensor component, biometric input of a user of the computing device over a duration of the security-sensitive operation;

comparing the repeatedly obtained biometric input to the securely-stored biometric information of the owner, wherein each of the comparisons comprises an authentication of the user; and

aborting the security-sensitive operation if the comparing step fails at any time over the duration of the security-sensitive operation.

104. A method of improving security of a computing device, comprising steps of:

operating a security component for the computing device, wherein the security component provides security functions such that the security component can vouch for authenticity of one or more other components with which it is securely operably connected;

providing a biometric sensor component that is securely operably connected, as one of the one or more other components, to the security component;

providing securely-stored biometric information which identifies an owner of the computing device;

repeatedly obtaining, from the biometric sensor component, biometric input of a user of the computing device; and

comparing the repeatedly obtained biometric input to the securely-stored biometric information of the owner.

105. A method of improving security of operations carried out with a computing device, comprising steps of:

operating a security component for the computing device, wherein the security component provides security functions such that the security component can vouch for authenticity of one or more other components with which it is securely operably connected;

providing a biometric sensor component that is securely operably connected, as one of the one or more other components, to the security component;

providing securely-stored biometric information which identifies an owner of the computing device;

performing a security-sensitive operation using the computing device;

repeatedly obtaining, from the biometric sensor component, biometric input of a user of the computing device over a duration of the security-sensitive operation;

comparing the repeatedly obtained biometric input to the securely-stored biometric information of the owner, wherein each of the comparisons comprises an authentication of the user; and

aborting the security-sensitive operation if the comparing step fails at any time over the duration of the security-sensitive operation.